JONES DAY | **Global Privacy & Cybersecurity Update**
Issue 12 | November 2016 JONES DAY

Jones Day Attorney Spotlight: Lisa Ropple

Cyberattacks remain among the most feared events that confront corporations. A significant data security incident can cripple a company's operations, damage its brand and relationships with customers or clients, expose the company to multiple regulatory investigations and lawsuits, and require substantial capital and human resources to address. Yet despite corporations' vigilant, material investments in defensive measures, industry researchers predict that cyberattacks will increase in both frequency and threat profile—targeted espionage, ransomware, denial of service, and privacy breaches. Some even predict that a major company will altogether collapse because of a security incident. Given these high stakes, responding effectively to a cyberattack is critical.

Lisa Ropple, a Boston-based partner in Jones Day's Cybersecurity, Privacy & Data Protection Practice, focuses her practice on helping companies respond effectively to significant data security events. She has represented clients in health care, financial services, retail, and other industries in connection with some of the largest public breaches in history. Experienced in all aspects of breach response, she

EDITORIAL CONTACTS

Daniel J. McLoon
Los Angeles

Mauricio F. Paez
New York

Jonathon Little
London

Kevin D. Lyles
Columbus

Todd S. McClelland
Atlanta

Jeff Rabkin
San Francisco

Adam Salter
Sydney

Michiru Takahashi
Tokyo

Undine von Diemar
Munich

Paloma Bru
Madrid

Olivier Haas
Paris

Jörg Hladjk
Brussels

Jay Johnson
Dallas

Editor-in-Chief: Anand Varadarajan

Practice Directory

HOT TOPICS IN THIS ISSUE

has structured and directed forensic investigations, worked with law enforcement authorities on criminal attacks, advised on notification obligations, and coordinated across internal corporate functions to facilitate a consistent, strategic response.

In addition, as a litigator for more than 25 years, Lisa represents companies in regulatory investigations and enforcement actions, including those brought by the FTC, SEC, OCR, state attorneys general, and other federal and state agencies.

United States

Regulatory—Policy, Best Practices, and Standards

NIST Publishes Trustworthy Email Guidance for Email Administrators
On September 21, the National Institute of Standards and Technology ("NIST") published a guidance document for email administrators and those developing security policies for enterprise email structures that provides recommendations for deployment and configuration of state-of-the-art email security technologies to detect and prevent phishing attacks and other malicious email messages. The guidance's abstract stated that the guideline applies to federal IT systems and will also be useful for small or medium-sized organizations.

NIST Issues Mobile Threat Guidance
On September 22, NIST issued guidance in response to the unique set of threats posed by mobile devices. The guidance discusses the NIST "Mobile Threat Catalogue," which describes, identifies, and structures the threats posed to mobile information systems and is designed to aid in protecting the connection between mobile devices and computer systems.

Ohio AG Launches CyberOhio Initiative
On September 29, the Ohio attorney general ("AG") discussed the launch of CyberOhio, a collection of initiatives aimed at helping Ohio businesses combat data security threats.

California AG Announces Cyber Crime Center Initiative
On October 10, the California AG announced the creation of the California Cyber Crime Center, known as C4, in Fresno. The initiative's stated purpose is to "investigate, prosecute, and prevent crime by harnessing the Department's expertise in cyber crime, cyber security, and digital evidence." As part of the new initiative, the AG also created a new unit

Introduction of Proposed Data Breach Notification Legislation

RECENT AND PENDING SPEAKING ENGAGEMENTS

For more information on Jones Day speaking engagements, please contact one of the editorial contacts listed above.

"Client Confidentiality in the Digital Age: Cybersecurity Ethics and Risk Mitigation for Lawyers," Houston Bar Association, Houston, Texas (January 12, 2017). **Jones Day Speakers**: Nicole Perry, Joshua Fuchs

"Blockchain," Development Institute International seminar, Paris, France (December 2). **Jones Day Speaker**: Olivier Haas

"Cybersecurity and Privacy Litigation Risks," Jones Day University, Columbus, Ohio (December). **Jones Day Speakers**: Jeff Rabkin, Todd Kennard, Richard DeNatale

"International Data Transfers, EU Standard Contractual Clauses, Privacy Shield," Frankfurt, Germany (November 28). **Jones Day Speakers**: Undine von Diemar, Jörg Hladjk

"Preparation for GDPR and Amended Personal Information Protection Act," Japan Pharmaceutical Industry Legal Affairs Association (November 11). **Jones Day Speaker**: Michiru Takahashi

"What You Should Know About EU Rules for International Data Transfer," Japan In-house Counsel Network (November 10). **Jones Day Speaker**: Michiru Takahashi

"Cyber Insurance for the Mortgage Finance Industry," webinar (November 10). **Jones Day Speaker**: Richard Milone

"The Data Protection Challenges of Analytics on Social Data," IAPP European Data Protection Congress, Brussels, Belgium (November 9). **Jones Day Speaker**: Olivier Haas

"Impact of the EU General Data Protection Regulation on Businesses," 16th Annual IDACON Conference, Munich, Germany (October 26). **Jones Day Speaker**: Jörg Hladjk

Privacy + Data Security Forum Panel

called the Office of Digital Investigations, as well as a "Cyber Accelerator" program to bring together members of various units to focus on research and development.

New Online Tool Helps Consumers Report California Online Privacy Protection Act Violations
On October 10, the California AG announced the release of an online form that allows consumers to report websites, mobile applications, and online services that are in violation of the California Online Privacy Protection Act. Operators of websites or applications could violate the Act by failing to post privacy policies or by posting incomplete or inadequate policies.

SEC OCIE Director Discusses Cybersecurity Examinations
On October 17, the director of the SEC's Office of Compliance Inspections and Examinations ("OCIE") delivered the keynote address at the National Society of Compliance Professionals 2016 National Conference. In discussing compliance improvement, the director mentioned that one of the OCIE's "larger upcoming initiatives" was "exams focusing on cybersecurity" and noted that such initiatives can provide companies with tools to use in their own compliance programs.

Regulatory—Critical Infrastructure

NIST Releases National Initiative for Cybersecurity Education ("NICE") Cybersecurity Workforce Framework
On November 2, NIST released the NICE Cybersecurity Workforce Framework ("NCWF") as a resource to allow U.S. employers to more effectively identify, recruit, develop, and maintain cybersecurity talent. The framework represents collaboration among government, industry, and academia, with the U.S. Departments of Defense and Homeland Security serving as significant contributors. NIST also announced its intention that the NCWF will serve as a building block to developing cybersecurity training standards.

Regulatory—Retail

Large-Scale Distributed Denial of Service Attack Affects Online Retailers
On October 21, a three-wave distributed denial of service ("DDoS") attack on domain name server "Dyn" resulted in multiple websites becoming unreachable or inoperable. The attack particularly affected numerous online retailers.

Regulatory—Defense and National Security

Presentation, George Washington University, Washington, D.C. (October 26). **Jones Day Speakers**: Mauricio Paez, Guillermo Larrea

"Cybersecurity: Managing Evolving Risks," Law School for the CFO, Orange County Chapter of CFO Leadership Council, Orange County, California (October 19). **Jones Day Speakers**: Edward Chang, Jessica Sawyer

"Big Data: At the Intersection of Competition and Privacy Laws," Belgian Federation of Enterprises, Brussels, Belgium (October 17). **Jones Day Speaker**: Laurent De Muyter

"What to Do in Case of a Cyber-Incident or Data Breach: How to Prepare for, and Avoid, a Crisis," Jones Day seminar, Amsterdam, The Netherlands (October 14). **Jones Day Speaker**: Jörg Hladjk

"EU Data Protection Reform: How to Escape Heavy Sanctions," RuSt Conference Business Circle, Austria (October 12). **Jones Day Speaker**: Jörg Hladjk

"Foreign Banks in Germany—New Challenges and New Chances," Outsourcing, IT and Data Protection VAB Seminar, Frankfurt, Germany (October 5–6). **Jones Day Speakers**: Undine von Diemar, Ted Kroke

"EU Privacy Laws and Implications for Implementing Health & Safety Programs," European Union Health, Safety & Environment Forum, Dublin, Ireland (September 28–29). **Jones Day Speaker**: Undine von Diemar

"The Debate Between Security and Privacy Continues: Where Do We Draw the Line?," ALM cyberSecure 2016, New York, New York (September 27). **Jones Day Speaker**: Mauricio Paez

"International Data Transfers: Accessing Your Organizations Adequacy," ALM cybersecure 2016, New York, New York (September 27). **Jones Day Speaker**: Mauricio Paez

"Cybersecurity and Insurance in the Age of Digital Vulnerability: What In-House Counsel Need To Know," Association of Corporate Counsel, San Diego, California (September 21). **Jones Day Speakers**: Jeff Rabkin, Richard DeNatale

"Eliminating the Weakest Link: Cybersecurity Ethics and Risk Mitigation for Lawyers," Jones Day CLE Breakfast Club, Houston, Texas (September 15). **Jones Day Speakers**: Nicole Perry, Joshua Fuchs

Air Force Launches Cyber Secure Campaign
On September 29, the Air Force chief information officer announced the establishment of the Chief Information Security Office and a year-long "Cyber Secure" campaign to address cybersecurity throughout the U.S. Air Force. The officer sent a memorandum to "all airmen" to highlight the vulnerability of Air Force systems to cyberattacks.

Department of Homeland Security Secretary Releases Statement on Recent DDoS Cyberattack
On October 24, the secretary of the Department of Homeland Security ("DHS") released a statement regarding the recent DDoS attack on domain name server "Dyn." The secretary identified malware that attacks Internet of Things devices such as surveillance cameras and entertainment systems as one type of malware potentially used in this incident. The secretary also stated that DHS has been working to develop a set of strategic principles for securing the Internet of Things, to be released in the near future.

Regulatory—Transportation

Court Grants Motion to Dismiss Action Against Transportation Network Company in FCRA Action
On October 5, the Northern District of California granted a motion to dismiss a complaint brought under the Fair Credit Reporting Act ("FCRA"), finding that the plaintiffs did not sufficiently plead standing. The case arose out of an alleged failure by the defendant transportation network company ("TNC") to provide clear disclosures that it would obtain its employees' credit and background reports. The defendant TNC moved to dismiss the complaint, arguing that the plaintiffs did not allege an injury in fact sufficient to grant Article III standing under the recent standard prescribed by the Supreme Court in *Spokeo, Inc. v. Robins*. The court agreed, finding that the plaintiff had not alleged a sufficient injury in fact and granting the motion to dismiss.

Regulatory—Financial Services

New York Governor Announces Cybersecurity Regulation to Protect Consumers and Financial Institutions
On September 13, the New York governor announced a regulation requiring banks, insurance companies, and other financial services institutions to "establish and maintain a cybersecurity program designed to protect consumers and ensure the safety and soundness of New York State's financial services industry." Regulated companies would have to annually certify compliance and designate an

"Binding Corporate Rules under the EU General Data Protection Regulation (GDPR)," IAPP KnowledgeNet, Munich, Germany (September 13). **Jones Day Speaker**: Jörg Hladjk

"What to Do When: You Get Hacked," Jones Day MCLE presentation, webinar (September 8). **Jones Day Speakers**: Jeff Rabkin, Greg Silberman, Richard DeNatale

"Eliminating the Weakest Link: Cybersecurity Ethics and Risk Mitigation for Lawyers," Jones Day CLE Breakfast Club, Houston, Texas (September 15). **Jones Day Speakers**: Nicole Perry, Jason Varnado

Enterprise Security Visibility Roundtable, CISO Executive Network, Atlanta Chapter: Atlanta, Georgia (September 8). **Jones Day Speaker**: Frances Forte

"Internet of Things, Civil Liabilities and Privacy," IAPP KnowledgeNet, Dallas, Texas (September 6). **Jones Day Speaker**: Jay Johnson

RECENT AND PENDING PUBLICATIONS

For more information on Jones Day's publications, please contact one of the editorial contacts listed above.

German Data Protection Authorities Initiate Review of International Data Transfers of 500 German Companies, Jones Day Publications (November). **Jones Day Authors**: Various

General Data Protection Regulation Guide, Jones Day Publications (November). **Jones Day Authors**: Various

Digital Health Law Update, Vol. II, Issue 5 (November 7). **Jones Day Authors**: Various

A New Sheriff in Town: Newly Regulated Broadband ISPs Get a First Look at FCC-Style Privacy Rules (November 7). **Jones Day Authors**: Mauricio Paez, Michael Hazzard, Bruce Olcott, Preston Thomas

Intra-Group Data Transfers under the Privacy Shield—Peculiarities and Solutions for the Practice, (*Konzerninterner Datentransfer unter dem Privacy Shield—Besonderheiten und Lösungsansätze für die Praxis*), Magazine of the German Association of Data Protection Officers (October). **Jones Day Author**:

internal cybersecurity officer. The regulation is subject to a 45-day notice and public comment period before final adoption.

G-7 Financial Leaders Endorse Bank Cybersecurity Best Practices
On October 11, Group of Seven ("G-7") financial leaders announced the release of bank cybersecurity best practices guidelines. The guidelines focus on banks' internal infrastructure and enhanced information sharing across banks and public-sector stakeholders, as well as the increased sophistication, frequency, and persistence of cyberattacks against banks.

Financial Regulators Outline Cybersecurity Standards
On October 19, the Department of the Treasury, the Federal Reserve Office of the Comptroller of the Currency, and the Federal Deposit Insurance Corporation issued a joint advance notice of proposed rulemaking regarding enhanced cyber-risk management standards for large and interconnected entities under their supervision and those entities' service providers. The proposed rulemaking addresses five categories of cyber standards: cyber-risk governance; cyber-risk management; internal dependency management; external dependency management; and incident response, cyber resilience, and situational awareness. The comment period runs until January 17, 2017.

Undine von Diemar

Post-Brexit: Privacy and Data Protection Issues in the UK (October 17). **Jones Day Author**: Jonathon Little

U.S. Government Streamlines Encryption Export Controls (October 12). **Jones Day Authors**: Various

Brexit: Implications for Data Protection and the General Data Protection Regulation in the UK (September 30). **Jones Day Authors**: Jonathon Little, Jörg Hladjk

"Keeping up with Self-Driving Vehicles," *Daily Journal* (September 23). **Jones Day Authors**: Jeff Rabkin, Todd Kennard, Brandy Ranjan

Regulatory—Health Care/HIPAA

HHS Issues Guidance on Cloud Computing and HIPAA
In October, the U.S. Department of Health and Human Services ("HHS") published guidance explaining obligations for covered entities and business associates when using cloud services providers under the Health Insurance Portability and Accountability Act ("HIPAA"). Under the guidance, when covered entities and business associates use cloud services, they must enter into an additional business associate agreement with the cloud services provider. Covered entities must also ensure that any service-level agreements in place with cloud service providers are consistent with the business associate agreements and applicable HIPAA rules.

Medical Center Settles Claims for Breach of Patient Information
In October, a large medical center in Southern California agreed to settle its claims with HHS for $2.1M following a breach of patient information. The claims arose out of the medical center's public posting of protected health information of more than 30,000 patients. This settlement follows a California state court's approval of a $39M settlement of consumer claims in March.

Litigation, Judicial Rulings, and Agency Enforcements

Large Internet Company Faces Class Actions for Breach of Consumer Information
In September 2016, three proposed class action lawsuits were filed in California and Illinois against a major internet company resulting from a 2014 breach of accountholder

information. This case stemmed from a leak of names, passwords, and other account information of at least 500M users. The company learned of the 2014 breach during the summer of 2016 and alerted users of the breach shortly thereafter. The complaint alleged that the company acted recklessly in securing its users' personal information and failed to discover the attack for "an unusually long time."

Eleventh Circuit Grants Stay of FTC Enforcement Order in Security Breach Case
On November 10, the United States Circuit Court of Appeals for the Eleventh Circuit granted a stay pending appeal of the Federal Trade Commission's ("FTC") enforcement order against a medical testing company. The FTC initially brought an action against the company for allegedly exposing the personal and billing information of more than 9,000 consumers on a peer-to-peer file-sharing network. The appeal presents the question of what types of harm in security breach cases qualify under the "unfairness" prong of the FTC act.

Vermont AG Reaches Settlement over Software Vulnerabilities
On October 12, Vermont's AG announced a settlement with software vendor Entrinsik, Inc. regarding vulnerabilities in its software related to a 2013 security breach at a Vermont college. Vermont's Consumer Protection Act requires vendors to eliminate software vulnerabilities or warn consumers about them. In a press release, the AG stated that "[t]his settlement is a warning to companies whose software introduce similar vulnerabilities."

Legislative—Federal

House Resolution Calls for National Strategy on Internet of Things
On September 12, the House of Representatives approved House Resolution 847, which urges the federal government to develop a national strategy to encourage the development of the Internet of Things and examine the connected technology's economic benefits and promotion of government efficiency. The resolution also calls on businesses to "implement reasonable privacy and cybersecurity practices" to protect consumers' sensitive data and increase their trust and acceptance of the industry.

House Passes Small Business Cybersecurity Aid Bill
On September 22, the House of Representatives passed the Improving Small Business Cyber Security Act, which authorizes the Small Business Administration ("SBA") to offer cybersecurity strategy grants to small business development centers that provide consulting services, guidance, and funding to small businesses and entrepreneurs. The grants would apply to independent businesses having fewer than 500 employees, which the SBA reports make up 99.7 percent of all the businesses in the United States.

House Passes Cybersecurity Government Data-Sharing Bill
On September 26, the House of Representatives passed the Cyber Preparedness Act to improve cyber-threat information-sharing and coordination between federal, state, and local authorities. The Act amends the Homeland Security Act of 2002 to require DHS to create a national cybersecurity coordination center and increase its responsibilities for coordinating between state and regional intelligence "fusion centers."

Senate Panel Probes FTC Data Security Enforcement and Authority
On September 27, members of the Senate Commerce, Science and Transportation Committee discussed the FTC's regulatory powers as applied to emerging data security issues. The FTC commissioners renewed their call for additional authority through federal legislation to set uniform data security and breach notification standards and give the commission the power to issue civil monetary fines.

Legislative—States

California's Amendment to Data Breach Notification Statute Takes Effect in January 2017

On September 13, California's governor signed A.B. 2828 into law, which amends California's breach notification law to require notification of a breach even if the personal information involved was encrypted. The bill will become effective on January 1, 2017.

The following Jones Day lawyers contributed to this section: Jeremy Close, Jay Johnson, Lindsey Lonergan, Alexandra McDonald, Dan McLoon, Mary Alexander Myers, Kelly Ozurovich, Mauricio Paez, Nicole Perry, Alexa Sendukas, John Sullivan, and Anand Varadarajan.

[Return to Top]

Latin America

Inter-American Development Bank and Organization of American States Publishes 2016 Report on Cyber Crime
This fall, the Organization of American States ("OAS") and Inter-American Development Bank published the 2016 Cyber Security Report for Latin America and the Caribbean. The report stated that the vast majority of Latin American countries are not yet prepared to counteract cybercrime. Utilizing surveys and other data provided by experts and officials from 32 OAS Member States, the report examined the cyber maturity of each of these countries by analyzing the following five topics: cybersecurity policy and strategy; cyber culture and society; cybersecurity education, training, and skills; legal and regulatory frameworks; and standards, organizations, and technologies.

Argentina

Congress Passes New Regulation of Access to Public Information
On September 14, the Argentine Congress passed a new regulation regarding Access to Public Information Decree no. 1172/2003 (source document in Spanish). The new law regulating this matter was published in the Official Gazette on September 29 as Law No. 27.275 (source document in Spanish). Per the new freedom of information regulation, individuals are entitled to request and receive from the government complete, adequate, accurate, and timely information regarding certain public affairs.

Brazil

Surveillance Companies Formalize Partnership in Brazil to Offer Cybersecurity Portfolio
On September 30, VERT and Suntech, two of the main cybersecurity and surveillance companies in Brazil, formalized a partnership (source document in Portuguese), for the optimization of client engagement, security intelligence, fraud management, and risk conformity products. The partnership offers global solutions in cybersecurity for Brazilian companies.

Colombia

Superintendence of Industry and Commerce Participates in Global Privacy Scan
On September 23, the Colombian Superintendence of Industry and Commerce participated in the Global Privacy Scan (source document in Spanish), organized by the Global Privacy Enforcement Network. The program examined approximately 300 devices related to Internet of Things (*Internet de las Cosas*), such as internet-connected thermostats and health monitor watches, in order to find out how producers informed consumers about the processing of personal data. The results indicated that six out of 10 Internet of Things devices do not properly disclose to consumers how their personal data will be used.

The following Jones Day lawyers contributed to this section: Guillermo Larrea, Elie Sherique, Daniel D'Agostini, and Mónica Peña Islas.

[Return to Top]

Europe

European Union

ECJ Finds Dynamic IP Addresses Constitute Personal Data
On October 19, the European Court of Justice ("ECJ") issued a decision recognizing that a website visitor's dynamic internet protocol ("IP") address constitutes personal data, as long as a website operator can obtain from an internet access provider additional information enabling the operator to identify the visitor. Previously, the ECJ held that IP addresses constituted personal data only with respect to internet access providers, which, unlike website operators, have access to both IP addresses and additional information enabling the identification of individuals.

Article 29 Working Party

Article 29 Working Party Reports on Priority Issues from Action Plan
On September 30, the Article 29 Working Party issued a report on a July Fablab workshop focused on operational and practical issues of the General Data Protection Regulation ("GDPR"). The workshop brought together European participants from various industries, civil society, and academics to discuss the priority issues identified in the Action Plan of the Working Party. These issues included the compliance toolbox aimed at making companies more responsible and accountable and the new right to portability, which strengthens citizens' rights.

European Data Protection Supervisor

EDPS Publishes Opinion on Enforcement of Fundamental Rights in Age of Big Data
On September 23, the European Data Protection Supervisor ("EDPS") issued Opinion 8/2016 on the enforcement of fundamental rights in the age of big data, which updated the 2014 Preliminary Opinion on Privacy and Competitiveness in the Age of Big Data. The updated opinion provides EU institutions with practical recommendations on how to apply the EU's objectives and standards more holistically. The Opinion addresses how concentration in digital markets might harm the interests of individuals as data subjects and consumers.

European Network and Information Security Agency

ENISA Publishes 2015 Annual Incident Report on Outage Incidents in Electronic Communications Sector
On October 5, the European Network and Information Security Agency ("ENISA") issued its annual report providing an aggregated analysis of the reports of significant outage incidents across the EU in 2015. The report discusses past incidents in the electronic communications sector in order to improve security in networks and services, and it provides an overview of impacted services and network assets and the root causes of the incidents.

Belgium

Privacy Commission Requires Cable Operator to Implement "Opt-in" Mechanism for Direct Marketing
On September 13, the Privacy Commission issued a press release (source documents in French and Dutch) about an ongoing investigation involving the direct marketing practices of a cable operator. Per the release, existing customers must be provided an opt-in mechanism, although the Privacy Commissions did not foreclose an opt-out

mechanism for new clients if appropriate transparency was ensured.

France

CNIL Analyzes Results of Connected Devices Audit
On September 23, the French Data Protection Authority ("CNIL") published an article (source document in French) discussing an international audit by 25 different national data protection authorities of more than 300 connected devices to assess their privacy impact. Among other findings, the audit results showed that the majority of connected devices did not provide clear and complete information regarding personal data collection and processing, data storage conditions, or modalities of personal data erasure.

CNIL Works on "Connected Vehicles" Conformity Pack
On October 3, CNIL published an article (source document in French) discussing the sixth conformity pack relating to "connected vehicles." Per the article, implementing the "personal data protection" dimension from the product design phase is critical to ensuring transparency and user control over data.

Digital Republic Law Takes Effect
On October 7, the Digital Republic Law was promulgated (source document in French), affecting CNIL's role and the rights of data subjects. The law increases the maximum amount of the administrative sanctions that may be imposed by CNIL from €150,000 to €3M. The law also creates a new right to be forgotten specific to minors and provides for an accelerated procedure to exercise this right. In addition, the law contains provisions relating to "digital death," which enables data subjects, during their life, to give instructions relating to the future of their personal data after their death.

French National Assembly Authorizes Personal Data Breach Group Actions
On October 12, the French National Assembly (*Assemblée Nationale*) adopted legislation enabling victims of personal data breaches to initiate group actions under certain conditions. To exercise these actions, victims need to be represented by an organization meeting the criteria provided by the bill. However, the bill allows for injunctive relief only and does not entitle group action participants to damages.

Germany

Data Protection Authority of North Rhine-Westphalia Publishes Privacy Shield Guidelines
On September 12, the North Rhine-Westphalia DPA published guidelines (source document in German) outlining responsibilities and requirements for transferring personal data from the EU to the United States under the new EU–US Privacy Shield. The guide, which is directed at data controllers, discusses due diligence requirements for transfers to Privacy Shield certified organizations, including certification verification and ensuring that the concrete data transfer is covered by the certification.

German DPAs Issue Guidance on Validity of Given Consents Under GDPR
On September 13 and 14, German DPAs issued a resolution (source document in German) that already-provided consents remain in force under the GDPR, as long as the manner in which consent has been given aligns with the conditions of the GDPR (Recital 171 of the GDPR). Specifically, the DPAs noted that given consents will no longer be effective if they do not comply with the prohibition of coupling (Article 7 (4) and Recital 43 GDPR) or do not respect the age limit of 16 (Article 8 (1) and Recital 33 GDPR).

Italy

Italian DPA Investigates Texting App
On September 27, the Italian DPA (*Garante per la protezione dei dati personali*) announced (source document in Italian and English) an investigation into privacy policy

changes made to a texting app's user accounts. In particular, the DPA seeks detailed information on: (i) data categories that the app is making available to a social media platform; (ii) mechanisms to obtain user consent; and (iii) how users can exercise their rights under Italian privacy legislation.

Code of Ethics for Processing Personal Data Takes Effect
On October 1, the Italian DPA's Code of Ethics and Conduct for Processing Personal Data for Business Information Purposes (source document in Italian) took effect. The adoption of the Code of Ethics, carried out in a joint effort with trade associations, is mandatory for all operators collecting data on companies' reliability and provides fixed principles for valid use of data banks and analysis instruments.

Spain

SDPA Sanctions Search Engine for Personal Data Communications Without Data Subject's Consent
On September 14, the Spanish Data Protection Agency ("SDPA") sanctioned a major search engine for violating data communication regulations because the search engine had not obtained user consent prior to transmitting information related to the right to be forgotten to the webmaster. The SDPA held that such transmission constituted a personal data communication, and therefore the consent of the data subject concerned was necessary.

SDPA Investigates Data Communication Between Two Main Social Networks
On October 5, the SDPA initiated (source document in Spanish) an ex officio preliminary inquiry proceeding to review whether data communications between social networks were in accordance with the Spanish data protection regulations. The SDPA proceeding will be coordinated with similar proceedings opened by other EU DPAs in the United Kingdom, Germany, and Italy.

SDPA and INCIBE Release Guide on Internet Privacy and Security
On October 7, the SDPA and Spanish Cybersecurity Institute ("INCIBE") published a Guide to Privacy and Security on the Internet (source document in Spanish). The Guide aims to provide internet users with practical guidelines to protect their personal information and to minimize risks. Tips include Wi-Fi network protection, phishing, managing cloud information, and how to set up profiles on social networks. Other public institutions collaborated in the production of the Guide, including the Spanish Police and the Spanish Health Ministry.

The Netherlands

DDPA Imposes Order on Wi-Fi Tracker
On September 1, the Dutch Data Protection Authority ("DDPA") issued a press release (source document in Dutch) stating that an order subject to penalty had been imposed on Wi-Fi tracker Bluetrace. The company provides Wi-Fi tracking technology that collects the media access control addresses of the devices of shop visitors via Wi-Fi signals. Although Bluetrace implemented a privacy policy, the DPPA found the policy violated the Dutch Data Protection Act.

DDPA Provides Guidance on Ransomware and Data Leaks
On October 3, the DDPA published (source document in Dutch) guidance regarding data involved in ransomware as part of its "Alert Online" campaign. Ransomware or cryptoware is a type of malicious software that infects a computer and restricts users' access until a ransom is paid to unlock it.

United Kingdom

English High Court Issues Subject Access Guidance

On September 23, the English High Court released a judgment providing further guidance on balancing competing rights when considering subject access requests. In its opinion, the Court emphasized the need for proper regard of privacy rights of individuals other than the person making the request.

Information Commissioner Speaks on Brexit
On September 29, in her first major speech since becoming UK Information Commissioner, Elizabeth Denham previewed UK data protection laws after Brexit and stated that the United Kingdom will need to adopt a new data protection law. She further stated that the new data protection law should be developed on an evolutionary basis to provide a degree of stability and clear regulatory messages for data controllers and the public.

ICO Issues Record Fine
On October 5, the Information Commissioner's Office ("ICO") issued a record fine of £400,000 for a major data breach by a UK mobile carrier. The carrier was subject to a "significant and sustained cyberattack" that led to the loss of more than 150,000 customers' data. The ICO found that the carrier had failed to take "appropriate technical and operation measures," focusing on outdated software and inadequate systems monitoring.

ICO Issues New Privacy Notice Code of Practice
On October 7, the ICO issued a new code of practice on privacy notices, including new guidance on the timing of notice to data subjects, and encouraged the use of privacy "dashboards" to provide greater choice for individuals.

UK Government to Penalize Firm Directors for Nuisance Calls
On October 23, the UK government announced it would adopt legislation under which firm directors can each be fined up to £500,000 by the ICO if they are found to be in breach of the Privacy and Electronic Communications Regulations. Prior to this announcement, only businesses were liable for fines for violations of these regulations.

The following Jones Day lawyers contributed to this section: Paloma Bru, Laurent De Muyter, Undine von Diemar, Olivier Haas, Jörg Hladjk, Bastiaan Kout, Martin Lotz, Giuseppe Mezzapesa, Evgenia Nosareva, Selma Olthof, Elizabeth Robertson, and Rhys Thomas.

[Return to Top]

Asia

People's Republic of China

China Adopts Cybersecurity Law
On November 7, China adopted a cybersecurity law in an attempt to counter the growing threats of hacking and terrorism. The law, which was passed by the standing committee of China's parliament, allows the government to act against domestic and foreign organizations that might harm Chinese national interests.

Hong Kong

PCPD Addresses Complaints Against Fitness Center's Proposal to Sell Membership Database
On September 26, the Hong Kong Privacy Commissioner for Personal Data ("PCPD") responded (source document in Chinese) to complaints lodged against a fitness center's proposal to sell its membership database. The response followed a warning (source document in Chinese) from the PCPD to fitness club members to "stay smart" in protecting their personal data.

Hong Kong to Host the 39th International Conference of Data Protection and Privacy Commissioners
On October 20, the PCPD promoted Hong Kong as the host of the 39th International Conference of Data Protection and Privacy Commissioners. The conference brings together hundreds of participants from around the world and is a global forum for 110 data protection authorities and trade and industry representatives.

Japan

Personal Information Protection Commission Releases Draft Guidelines Regarding Amended Personal Information Protection Act
On October 4, the Personal Information Protection Commission released draft Guidelines Concerning Personal Information Protection Act (General Rules) (source document in Japanese) for public comments. The Commission aimed to unify existing ministerial guidelines under these new procedures and also released a set of specific draft guidelines, including: (i) draft guidelines regarding the provision of personal data to a foreign third party; (ii) draft guidelines regarding verification and documentation obligations related to the transfer of data to third parties; and (iii) draft guidelines regarding de-identified information (all source documents in Japanese).

Cabinet Releases Enforcement Cabinet Order of Personal Information Protection Act
On October 5, after a review of public comments, the Cabinet released (source document in Japanese) the Enforcement Cabinet Order of the Personal Information Protection Act. Notably, the order defines the term "Individual Identification Code," which is a category of personal information spanning DNA data, finger or palm print data, passport number, or driver's license number.

Personal Information Protection Commission Releases Enforcement Regulation of Personal Information Protection Act
On October 5, after review of public comments, the Personal Information Protection Commission released (source document in Japanese) the Enforcement Regulation of Personal Information Protection Act. The enforcement regulation provides rules for creating and using de-identified information, obligations to verify and document transfer of personal data, and safeguards for extraterritorial data transfer.

Singapore

PDPC Assesses S$25,000 Penalty for Breach of Protection Obligation
On September 21, Singapore's Personal Data Protection Commission ("PDPC") found that Toh-Shi Printing Singapore failed to implement proper and adequate procedural checks while processing personal data for Aviva Ltd., resulting in the unauthorized disclosure of personal data of more than 8,000 Aviva policyholders. The Commission imposed a financial penalty of S$25,000 for violating the Personal Data Protection Act of 2012.

PDPC Issues S$3,000 Penalty for Breach of Protection Obligation
On September 30, the PDPC ruled that GMM Technoworld Pte. Ltd., a waterproof gadget retailer, failed to implement proper and adequate security measures on its website, resulting in an unauthorized public disclosure of approximately 129 customers' personal data. The Commission assessed a penalty of S$3,000 for violating the Personal Data Protection Act.

PDPC Sanctions Food Caterer for Breach of Protection Obligation
On November 4, Singapore's PDPC found that Smiling Orchid Pte. Ltd., a food caterer, failed to make reasonable security arrangements to prevent unauthorized access to its customers' personal data on its website, and the PDPC imposed a S$3,000 penalty for violating the Personal Data Protection Act of 2012. The PDPC noted that users were able to access other customers' personal data by altering the URL of their order preview

webpage. The PDPC also directed Smiling Orchid to conduct a security audit and to patch all identified webpage vulnerabilities.

Taiwan

Ministry of Justice Issues an Announcement
On September 2, the Ministry of Justice announced that the police may use the Advanced Passenger Information System to collect certain types of data on passengers, including nationality, place of arrival, place of departure, and PN Recode, while investigating drug-related crimes.

The following Jones Day lawyers contributed to this section: Michiru Takahashi and Li-Jung Huang.

[Return to Top]

Australia

Australian Information Commissioner Issues Fine for Privacy Breach
In September, the Australian Information Commissioner fined Comcare for improperly disclosing an employee's personal information to the employee's former employer and insurer. The Commissioner determined that Comcare had breached Australian Privacy Principles by failing to obtain the individual's consent to the disclosure and by failing to take reasonable steps to protect the information from unauthorized disclosure. The Commissioner ordered Comcare to review and report on its quality assurance procedures, and the employee was awarded AU$3,000 in damages.

Introduction of Proposed Data Breach Notification Legislation
On October 19, the Australian government introduced proposed legislation to create a mandatory data breach notification scheme. The proposed legislation would require entities to notify the Australian Information Commissioner and affected individuals of "eligible data breaches" where there is likely unauthorized access or disclosure of information that could result in serious harm to any of the individuals to whom the information relates. The bill is scheduled for a second reading in the Lower House of Parliament.

The following Jones Day lawyers contributed to this section: Adam Salter, Peter Brabant, and Nicola Walker.

[Return to Top]

Jones Day Cybersecurity, Privacy, and Data Protection Lawyers

Emmanuel G. Baud Paris	Po-Chien Chen Taipei	Shawn Cleveland Dallas	James A. Cox Dallas
Walter W. Davis Atlanta	Timothy P. Fraelich Cleveland	Joshua L. Fuchs Houston	Karen P. Hewitt San Diego
John E. Iole Pittsburgh	Robert W. Kantner Dallas	Elena Kaplan Atlanta	Jeffrey L. Kapp Cleveland
J. Todd Kennard Columbus	Ted-Philip Kroke Frankfurt	Jonathan Little London	Kevin D. Lyles Columbus
John M. Majoras Columbus/Washington	Todd S. McClelland Atlanta	Kristen P. McDonald Atlanta	Carmen G. McLean Washington

Daniel J. McLoon
Los Angeles

Caroline N. Mitchell
San Francisco

Matthew D. Orwig
Dallas

Mauricio F. Paez
New York

Chaka M. Patterson
Chicago

Nicole M. Perry
Houston

Jeff Rabkin
San Francisco

Lisa M. Ropple
Boston

Adam Salter
Sydney

Gregory P. Silberman
Silicon Valley

Cristiana Spontoni
Brussels

Michiru Takahashi
Tokyo

Rhys Thomas
London

Michael W. Vella
Shanghai

John A. Vogt
Irvine

Sergei Volfson
Moscow

Undine von Diemar
Munich

Toru Yamada
Tokyo

Sidney R. Brown
Atlanta

Paloma Bru
Madrid

Laurent De Muyter
Brussels

Bénédicte Graulle
Paris

Olivier Haas
Paris

Jörg Hladjk
Brussels

Jay Johnson
Dallas

Guillermo E. Larrea
Mexico City

Christopher J. Lopata
New York

Margaret I. Lyle
Dallas

Giuseppe Mezzapesa
Milan

Jérémy Attali
Paris

Laura Baldisserra
Milan

Peter Brabant
Sydney

Nigel Chin
Singapore

Jeremy S. Close
Irvine

Daniel C. D'Agostini
São Paulo

Steven G. Gersten
Dallas

Bart Green
Irvine

Jan Grootenhuis
Amsterdam

Aaron M. Healey
Columbus

Bastiaan K. Kout
Amsterdam

Lindsey Lonergan
Atlanta

Martin Lotz
Munich

Alexandra A. McDonald
San Francisco

Evgenia Nosareva
Paris

Selma Olthof
Amsterdam

Kelly M. Ozurovich
Los Angeles

Mónica Peña Islas
Mexico City

Brandy H. Ranjan
Columbus

Jessica M. Sawyer
Los Angeles

Alexa L. Sendukas
Houston

Elie J. Sherique
São Paulo

John T. Sullivan
Dallas

Raquel Travesí
Madrid

Anand Varadarajan
Dallas

Nicola Walker
Sydney

Natalie A. Williams
Atlanta

Follow us on:

Jones Day is a legal institution with more than 2,500 lawyers on five continents. We are One Firm Worldwide[SM].